(12) UK Patent Application (19) GB (11) 2 122 777 A

(21) Application No 8217456
(22) Date of filing 16 Jun 1982
(43) Application published 18 Jan 1984
(51) INT CL[3] G06F 13/00 5/00
(52) Domestic classification G4A AP
(56) Documents cited
EP A 0008033
WO 81/2351
US 4262329
(58) Field of search G4A

(71) Applicant
Open Computer Services Limited,
(United Kingdom),
Aqua House,
24—25 Old Steine,
Brighton,
East Sussex,
BN1 1EL

(72) Inventor
David B. Everett

(74) Agent and/or address for service
Withers and Rogers,
4, Dyer's Buildings,
Holborn,
London,
EC1N 2JT

(54) Software protection apparatus and method

(57) Apparatus for preventing the unauthorised copying of or tampering with software in a computer makes use of a tamper-resistant module (1) for decrypting an encrypted program in the computer memory (4). The tamper-resistant module includes a microprocessor (2) and decryption circuitry which together operate to decrypt and execute the program instruction by instruction in real time. The decryption circuitry includes a first memory for storing a decryption key and decryption algorithms, and a second memory for temporarily storing a memory map generated inside the tamper-proof module when a decryption key, prefixed to the encrypted program, is received. Elements of the memory map correspond to locations in the computer memory (4) and are individually combined with respective instructions in the program as they are read out of the computer memory, each instruction being decrypted in this way and then executed in the processor (2) before the next instruction is processed. The apparatus is also capable of decrypting a key which is itself in encrypted form, using for example a public key system. Advantages of the apparatus are that the decrypted program does not appear on conductors outside the tamper-resistant module, and that once the memory map has been generated, the program can be decrypted and executed in real time at a relatively fast rate.

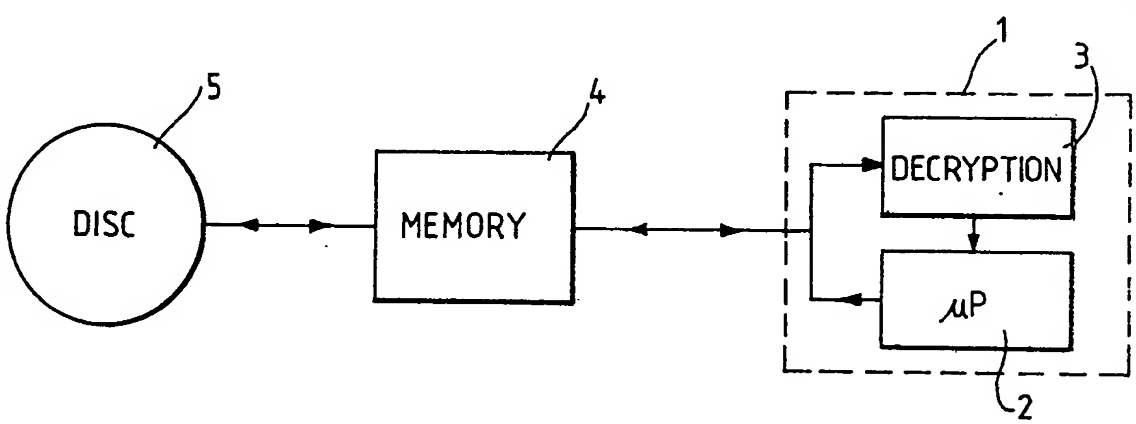


Fig.1.

The drawings originally filed were informal and the print here reproduced is taken from a later filed formal copy.

GB 2 122 777 A

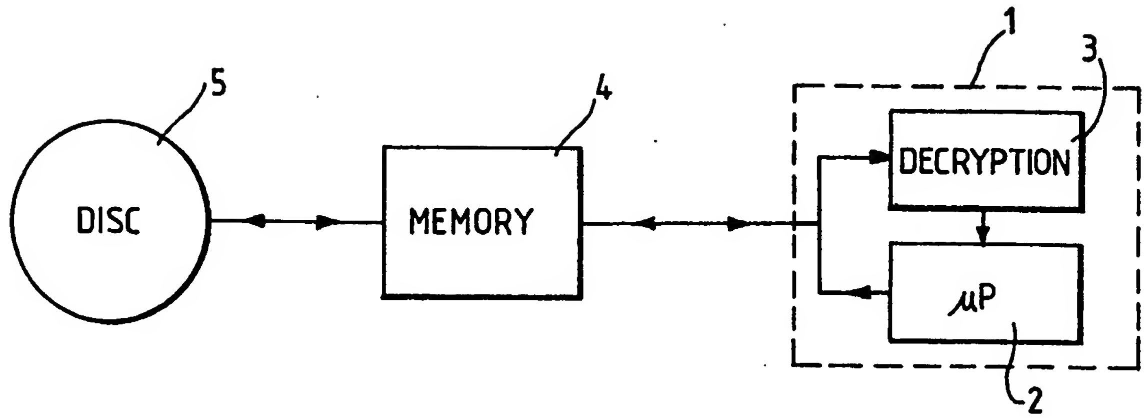

5
DISC
4
MEMORY
1
3
DECRYPTION
μP
2

Fig.1.

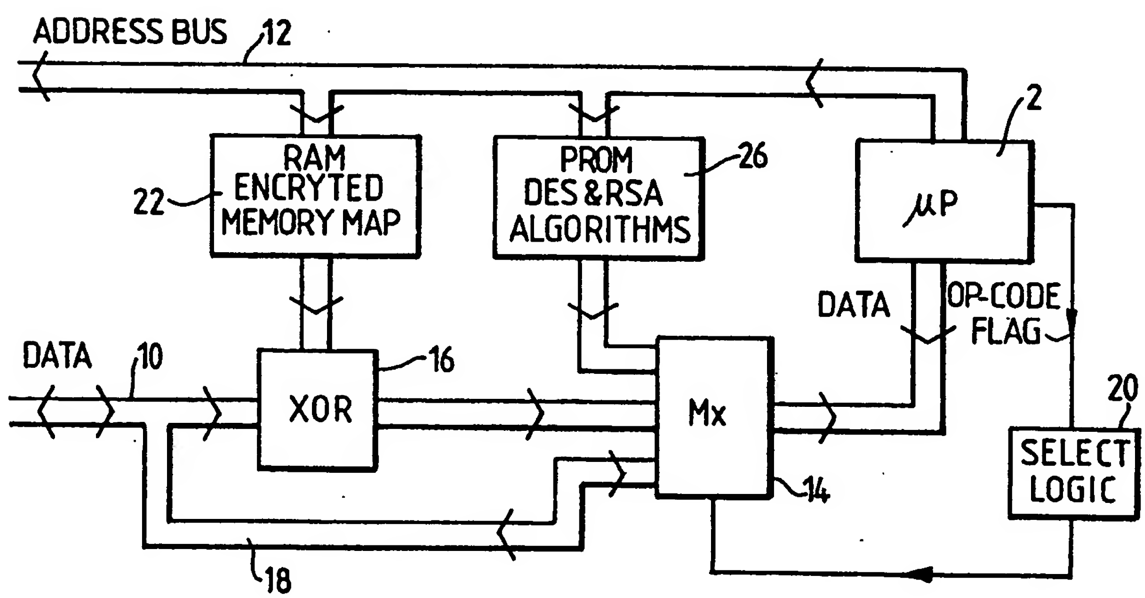

ADDRESS BUS
12
2
RAM
ENCRYTED
MEMORY MAP
22
PROM
DES & RSA
ALGORITHMS
26
μP
DATA
OP-CODE
FLAG
DATA
10
XOR
16
Mx
14
20
SELECT
LOGIC
18

Fig.2.

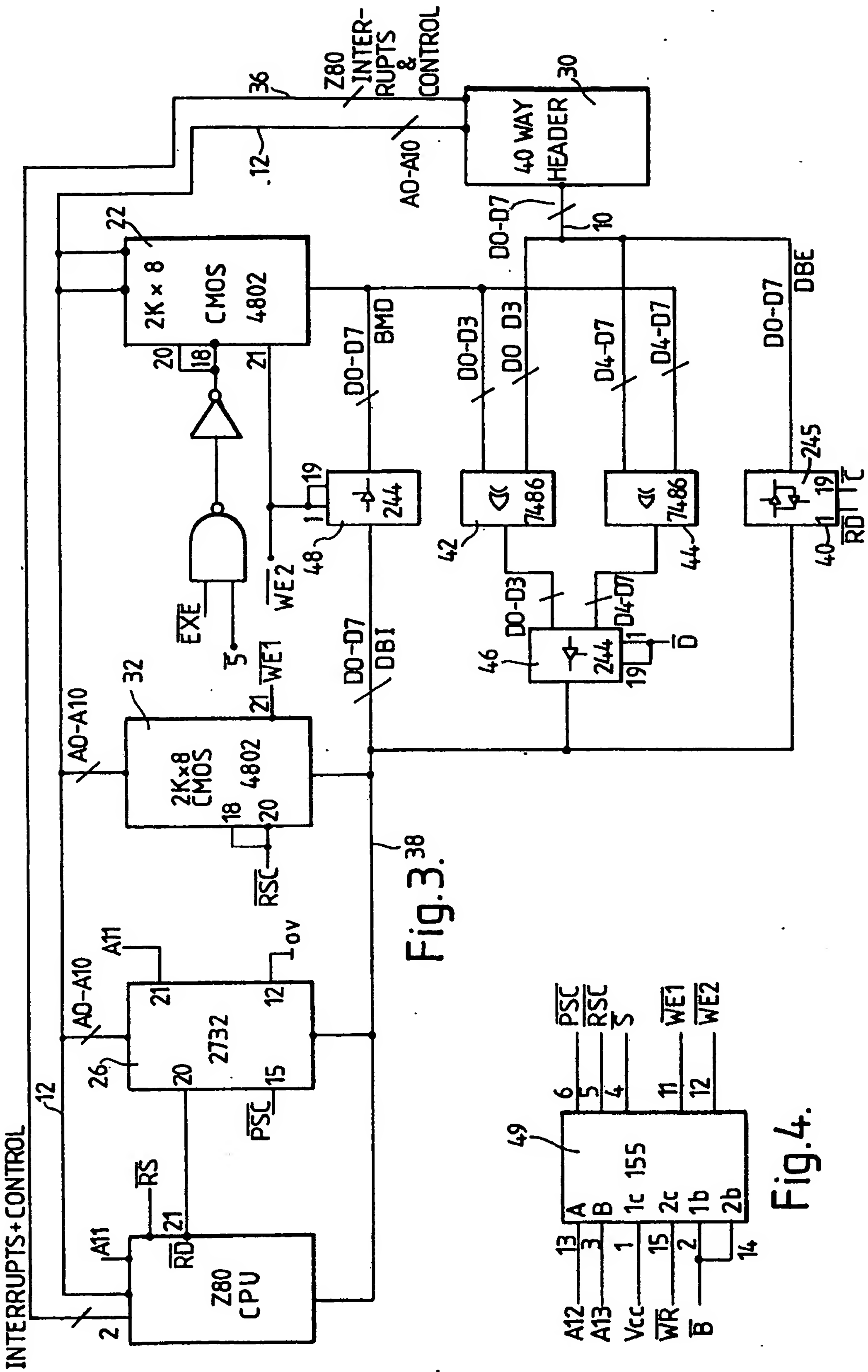
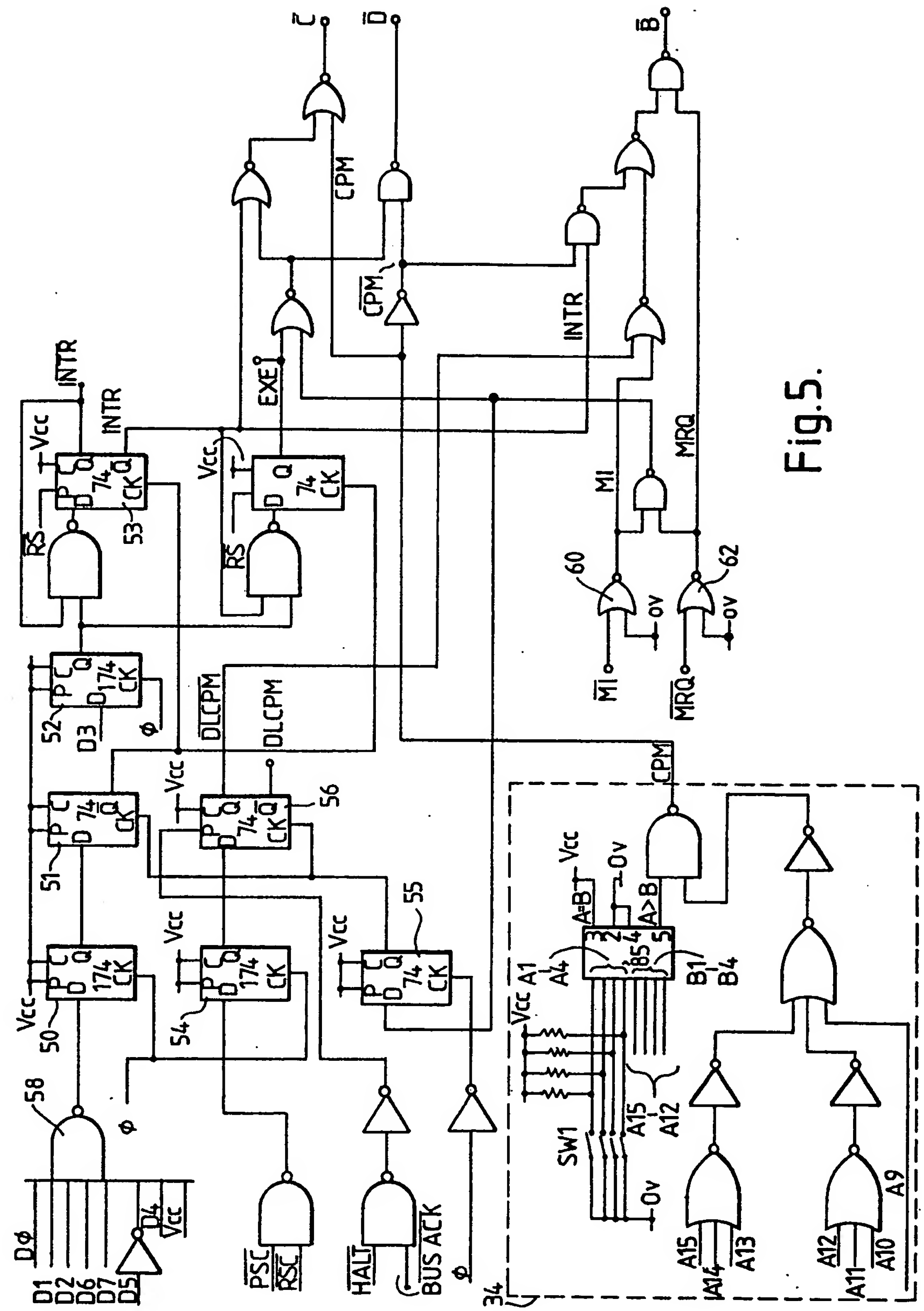

INTERRUPTS+CONTROL
Z80 CPU
2
A11
RD
21
RS
12
AO-A10
26
2732
20
21
15
12
PSC
A11
OV
32
2K×8 CMOS 4802
18
20
RSC
21
WE1
38
DO-D7
DBI
EXE
S
WE2
48
244
1
19
22
2K × 8 CMOS 4802
36
Z80 INTER-RUPTS & CONTROL
AO-A10
30
40 WAY HEADER
DO-D7
10
BMD
DO-D3
DO D3
D4-D7
DBE
42
7486
44
46
245
40
RD
C
D
49
155
A12
A13
Vcc
WR
B
13
3
1
15
2
14
A
B
1c
2c
1b
2b
6
5
4
11
12
PSC
RSC
S
WE1
WE2

Fig.3.

Fig.4.



C̄
D̄
B̄
CPM
C̄P̄M̄
INTR
EXE
MI
MRQ
M̄Ī
M̄R̄Q̄
60
62
0v
Vcc
R̄S̄
74
174
CK
53
52
D3
DLCPM
D̄L̄C̄P̄M̄
51
56
55
50
54
58
Dϕ
D1
D2
D6
D7
D5
D4
P̄S̄C̄
R̄S̄C̄
H̄ĀL̄T̄
BUS ACK
ϕ
34
SW1
A1
A4
A15
A12
B1
B4
85
A=B
A>B
A14
A13
A11
A10
A9

Fig.5.

SPECIFICATION

Software protection apparatus and method

This invention relates to apparatus and a method for inhibiting the unauthorised copying of or tampering with computer software. It is directed primarily to the protection of programs for industrial and business use.

The increasing use of microprocessors in equipment for industry and commerce has implications not only on the design of hardware but also the distribution and storage of software packages. The problem of protecting software from 'piracy' is particularly important in view of the increasing proportion of relatively small systems having for example two or three monitors and the consequent potential for unauthorised copying. Whilst advantages in the compatibility of systems are important for a software supplier, 'piracy' either aggressively or through more passive associations seriously limits the returns that the supplier may expect to gain.

Two principal methods have been applied to the problem of protecting software in an attempt to limit copying activities. The first is to make the copying of data from discs difficult to implement, but this has the disadvantage for the user who may then be unable to take back-up copies of his programs. Secondly, a number of modifications can be made to the computer hardware so that the software will only execute correctly if the appropriate response is received from the hardware. In the simplest case this may be a register that is read by the system to confirm some unique code, or in more complex cases may involve a set of instructions that actually define sequences in the copying process. Whilst both methods may deter the bona fide business user, they would be unlikely to prevent more determined efforts from succeeding.

It is an object of this invention to provide a device and a method for inhibiting the unauthorised copying of stored computer programs largely without preventing an authorised user from taking back-up copies for his own use.

According to a first aspect of this invention, there is provided computer data processing apparatus including a memory and a central processing unit for executing a program stored in the memory, characterised in that the processing unit is connected to decryption means, the said decryption means and the processing unit or part thereof comprising a tamper-resistant module. To take an embodiment of this invention as applied to a microcomputer, the tamper-resistant module preferably comprises an integrated or sealed unit including together a microprocessor and decryption circuitry arranged specifically to decipher incoming data signals encrypted in a particular way. The tamper-resistant module is connected to the memory in the same way that a microprocessor is connected to the memory in a standard microcomputer, and can be so designed that it may be used as a direct plug-in replacement for the microprocessor integrated circuit in the standard microcomputer when the microcomputer is to be used for executing encrypted programs.

By bringing the processing unit and decryption circuitry together in a tamper-resistant module and providing the user with an encrypted program, the program can be executed in the computer without the decrypted program appearing in the memory or on accessible electrical conductors. It can thus be arranged that the decrypted program exists only inside the tamper-resistant module where it is inaccessible to copying.

According to a second aspect of the invention a device for inhibiting unauthorised copying of or tampering with computer programs comprises a tamper-resistant module for replacing a central processing unit in a computer, wherein the module includes a processing unit, a decryption circuit, a data bus, and address bus for connection to an external memory unit in the computer.

According to a third aspect of the invention a method of inhibiting the copying or tampering with computer programs in a computer designed to execute such programs comprises: storing a program in a memory in the computer in encrypted form, and executing the said program by feeding it instruction by instruction to a tamper-resistant module including a central processing unit and a decryption device.

In a preferred embodiment of the invention, the tamper-resistant module contains a microprocessor chip and a RAM (random access memory) memory map. The protected software is supplied to the user encrypted using the DES algorithm, with the key to the DES algorithm prefixed to the software in encrypted form using the RSA Public Key system. The Public Key is uniquely defined for the particular tamper-resistant module contained in the user's computer. (For a description of encryption and decryption using the DES algorithm, see Federal Information Processing Standards (FIPS) publication 46 "Data Encryption Standard" published January 1977. The RSA Public Key system is disclosed in "A Method for Obtaining Digital Signatures and Public Key Cryptosystems" by Rivest, Shamir and Aldeman — Communications of the Association for Computing Machinery, February 1978). In operation the DES key is loaded into the tamper-resistant module and decrypted. The decrypted key is then used in the DES algorithm to generate a local memory map in the RAM corresponding to at least a portion of a memory external to the module. When an encrypted program is fed into the module from the external memory, each op-code is exclusive-OR'ed with the corresponding code in the memory map to decrypt the op-code before presentation to the microprocessor chip. The tamper-resistant module can be arranged to recognise an incoming encrypted program to put the above decryption operation into effect, or alternatively to by-pass the exclusive-OR

function when the incoming program is not recognised as being encrypted.

The invention will now be described by way of example with reference to the drawings in which:—

Fig. 1 is a simplified block diagram of apparatus in accordance with one aspect of the invention;

Fig. 2 is a block diagram of a tamper-resistant module;

Fig. 3 is a circuit diagram of part of the tamper-resistant module showing a microprocessor, memory devices, a combining circuit and signal switching devices;

Fig. 4 is a circuit diagram of a memory selector circuit in the tamper-resistant module; and

Fig. 5 is a circuit diagram of decryption select logic.

Referring to Fig. 1 a system in accordance with the invention in a simplified form comprises a tamper-resistant unit 1 including a central processing unit (c.p.u.) 2 (in this case a microprocessor) and decryption means 3. The tamper-resistant unit 1 replaces the c.p.u. of a conventional computer, and like a conventional c.p.u., is connected to a system memory 4 which transfers program op-codes and data to and from the c.p.u. Permanent storage of programs and data is provided in this embodiment by a disc store 5. In operation of the system an encrypted program and data is loaded into the memory 4 from the disc store 5 and then fed instruction by instruction to the decryption means 3 and the c.p.u. 2. Preferably, only the op-codes are encrypted, since this makes the program relatively secure from cryptanalysis.

The tamper-resistant module 1 is shown in more detail in Fig. 2. The module is connected to the system memory by a data bus 10 and an address bus 12. Signals transmitted from the memory to the module on the data bus pass to the microprocessor c.p.u. via a switching means 14 either through an exclusive-OR (XOR) combiner stage 16 or via a bypass connection 18 in response to signals from select logic circuitry 20. The XOR stage 16 is also connected to an internal RAM 22 the purpose of which will be described below. Thus, signals on the data bus 10 entering the XOR stage 16 are combined in an exclusive-OR process with signals from the internal RAM 22, the resultant signals then passing along an internal data bus 24 to the c.p.u. The data inputs of the c.p.u. can also receive signals from a third source via the switching means 14, this being an internal PROM 26 which contains a program or programs for controlling decryption operations. The PROM 26, the internal RAM 22 and the external memory 4 are connected to the c.p.u. 2 by the common address bus 12. The function of these elements will become clear from the following description of the decryption process.

The preferred encryption method which is applied by the software supplier to the programs delivered to the user is that described in the Data Encryption Standard (DES) referred to in the introduction to this specification. In this method, the same algorithm (the 'DES algorithm') is used both to encrypt and decrypt the message. The algorithm is well known, but successful deciphering depends on knowledge of a key (the 'DES key') which was used in the algorithm to encrypt the message. In the present system the program op-codes are encrypted by the software supplier or dealer using the DES algorithm and a particular DES key. To transmit the DES key in a secure manner to the user, it is prefixed to the program in an encrypted form using a second encryption process. This second encryption process is carried out according to the RSA method also referred to in the introduction.

In the RSA method, the message (in this case the DES key) is encrypted by a mathematical operation using a public encryption key which is associated with the recipient, i.e. the DES key is encrypted using the user's public key. Decryption can only be carried out by a private decryption key which cannot be derived from the public key. The private key is stored in the tamper-resistant module, in a second internal RAM 32 which is powered by a small battery.

Referring again to Fig. 2, when an encrypted program is fed to the tamper-resistant module, the DES key is first decrypted by the c.p.u. 2 working in accordance with an RSA decryption program stored in the PROM 26. Further execution of the main encrypted program is then delayed while the DES key is used in the DES algorithm to generate a local memory map in the RAM 22 under the control of a further program in the PROM 26. This operation complete, the DES encrypted program is then run with each op-code being subjected to an exclusive-OR operation in which it is combined with a mapped code from a location in the RAM 22 corresponding to the location of the op-code in the system memory 4 (Fig. 1). The result of the exclusive-OR operation is a decrypted op-code which passes through the switching means 14 to the c.p.u. instruction register. It should be noted that at no time does the decrypted op-code appear outside the tamper-resistant module. If the user wishes to make a back-up copy of the program, it is the encrypted program which is reproduced.

In the decryption process described above the DES is used in the cipher feedback mode in order to remove pattern repetition from the memory map. By generating the memory map before the program is run, decryption is carried out in two stages, a first stage which is not time-critical, and a second stage (the exclusive-OR operations) which is comparatively trivial and can be implemented in real time consistent with the normal clocking rate of the c.p.u.

Figs. 3, 4 and 5 are circuit diagrams of a tamper-resistant module in accordance with the invention. The circuit includes a number of individual integrated circuit chips but it should be understood that a circuit carrying out similar functions could be built into one or two purpose-

designed LSI chips to reduce unit costs in large scale manufacture.

The circuit shown is designed to be mounted as a sealed container inside an existing or new computer as a replacement for the Z80 microprocessor. The module is capable of retroactive refit, and for this purpose has a 40-way header plug 30 (Fig. 3) for connection with the standard 40-way microprocessor socket.

A number of subsidiary features of the circuit which do not appear in the block diagram of Fig. 2 include the provision of storage space in the second internal RAM 32 for use during execution of the RSA and DES algorithms, and a decoding circuit 34 (Fig. 5) for by-passing the decryption circuitry when accessing portions of the external memory containing CP/M operating system pointers.

Referring firstly to Fig. 3, the illustrated part of the circuit contains virtually all of the circuitry associated with the blocks of Fig. 2 with the main exception of the select logic circuitry 20. The 40-way header plug 30 brings in the system data bus 10, address bus 12 and the Z80 interrupt and control lines.

Signals entering the tamper-resistant module on the external data bus 10 are transmitted to an internal data bus 38 either directly via a transceiver device 40 or via a parallel pair of exclusive-OR combining devices 42 and 44 and a tri-state buffer switch 46. Transmission via exclusive-OR gates 42 and 44 occurs in response to input $\overline{D}$ on buffer 46 being active. This happens when the incoming signal is an encrypted op-code during execution of the main program. At other times during execution of the main program signals pass freely between the external data bus 10 and internal data bus 38 via transceiver 40 in response to an active input $\overline{C}$.

Prior to decrypting an incoming main program, it is necessary to decrypt the incoming DES key and generate the DES memory map in the first internal RAM 22. The programs for these operations are stored in PROM 26. Thus, initially the c.p.u. 2 executes internal programs in conjunction with PROM 26 and second RAM 32 without accessing the external memory. During this operation the RSA private key is looked up in the RAM 32 and the DES key decrypted. The DES is then used with the DES algorithm stored in the PROM to build up the DES memory map in the first RAM 22 via buffer 48.

Once the memory map has been established, the main program can be run in the c.p.u. 2, the contents of the memory map being exclusive-OR'ed with incoming op-codes in gates 42 and 44.

Routing of signals on the data buses is controlled by the circuitry of Figs. 4 and 5. Fig. 4 shows a one-of-four selector device 49 for selecting and controlling the memory chips 26, 32 and 22 in response to address lines A12 and A13 (internal RAM/PROM select), an op-code detect signal $\overline{B}$ from op-code detect circuitry (Fig. 5), and a write signal $\overline{WR}$ from the c.p.u. 2.

The select logic circuitry in Fig. 5 includes an array of flip-flops 50 to 56 controlling the generation of interrupt signals INTR and $\overline{INTR}$ which are fed to the c.p.u. 2 when an incoming encrypted program is signalled. Generation of the interrupt signal causes the c.p.u. 2 to enter the internal program loop for generating the memory map. In this example it is assumed that an encrypted program will be prefixed by a restart instruction which is detected by AND gate 58. However, any suitable recognition signal may be used in conjunction with means for detecting the signal.

The existence of an op-code on the data bus is signalled by the c.p.u. 2 to OR-gates 60 and 62 which activate output $\overline{B}$ (connected to selector device 49 in Fig. 4) and output $\overline{D}$ (connected to buffer 46 in Fig. 3) to select the decrypt operation.

Flip-flop 56 preset input is coupled to the microprocessor $\overline{HALT}$ and $\overline{BUSACK}$ outputs as a safeguard against possible interference with the c.p.u. 2 in an attempt to read out decrypted signals.

The address decoding circuit 34 detects accessing of addresses in memory associated with the CP/M operating system, and generates an output CPM for by-passing the decryption circuitry.

Claims (filed 13/6/83)

1. Computer data processing apparatus including a memory and a central processing unit for executing an encrypted program stored in the memory, characterised in that the processing unit is connected to decryption means, the decryption means and at least a part of the processing unit comprising a tamper-resistant module.

2. Apparatus according to claim 1, wherein the processing unit is a microprocessor.

3. A device for inhibiting unauthorised copying of or tampering with computer programs, comprising:

a tamper-resistant module at least part of a processing unit, a decryption circuit, and data and address busses for connection to an external memory.

4. A device according to claim 3, wherein the tamper-resistant module is arranged to execute encrypted instructions of a program fed to the module from the data bus.

5. Computer data processing apparatus for executing an encrypted computer program, comprising:—

a program memory for storing the encrypted program and a decryption key;

a central processing unit for executing the program;

a decryption circuit;

a data bus coupling the program memory to the decryption circuit; and

an address bus coupling the processing unit to the program memory;

the decryption circuit and at least part of the processing unit forming part of a tamper-resistant module;

wherein the decryption circuit includes a first decryption memory for storing a decryption algorithm, a second decryption memory for storing a decrypted copy of the program.

6. Apparatus according to claim 5, wherein the decrypted copy is a memory map having elements corresponding to program storage locations in the program memory, and wherein the apparatus includes combining means having an input coupled respectively to the data bus and the second decryption memory and an output coupled to the processing unit.

7. Apparatus according to claim 6, wherein the decryption circuit further includes a switching device coupled to the data bus for routing signals from the program memory to the processing unit so that the combining means is by-passed.

8. Apparatus according to claim 7, wherein the switching device has a control input coupled to an output of the processing unit for routing signals through the combining unit only when the signals represent a program instruction.

9. Apparatus according to claim 5, wherein the first decryption memory is a read only memory having a decryption program stored therein for generating the decrypted copy of the encrypted program using the said decryption key and the decryption algorithm.

10. Apparatus according to claim 6, wherein the combining means is operable to combine signals on the data bus with elements of the memory map by a reversible logic operation.

11. Apparatus according to claim 10, wherein the reversible logic operation is an exclusive-OR operation.

12. Apparatus according to claim 5, including means for decrypting the decryption key when the latter is itself in encrypted form in the program memory, the decryption circuit including means for storing a private auxiliary decryption key, means for recognising a public auxiliary encryption key in incoming signals, which public key is mathematically related to the private key, and means for decrypting the encrypted decryption key prior to generating the decrypted program copy.

13. Apparatus according to claim 12 arranged to decrypt the program using the DES Data Encryption Standard, and to decrypt the DES decryption key using the RSA Public Key system.

14. Apparatus according to claim 5, wherein the decryption circuit is arranged to decrypt the encrypted program such that the program can be run in real time, each program instruction being decrypted and fed to the processing unit for execution.

15. A method of inhibiting the copying of or tampering with computer programs in a computer designed to execute such programs, comprising the steps of:

storing a program in a memory in the computer in encrypted form, and

executing the program by feeding instructions in the program to a tamper resistant module including at least a part of a processing unit and a decryption device.

16. A method of inhibiting the copying of or tampering with a computer program in a computer designed to execute such programs, comprising the steps of:—

providing, in the computer, a tamper-resistant module containing a processing unit, or at least a part thereof, and decryption circuitry including a first decryption memory;

encrypting a program using an encryption key;

storing the encrypted program and the key in a memory in the computer, which memory is external to the tamper-resistant module;

feeding the key and the encrypted program from the external memory to the tamper-resistant module and generating therefrom a decrypted copy of the program in the first decryption memory using the key;

feeding the encrypted program to the tamper-resistant module to decrypt the program; and

executing the decrypted program in the real time in the processing unit;

electrical signals representing the decrypted program being confined to electrical elements inside the tamper-resistant module.

17. A method according to claim 16, wherein the decrypted program copy comprises a decryption memory map in the first decryption memory, and wherein the encrypted program is combined with the memory map, increments of the encrypted program being fed sequentially to the combining means, each individual increment being combined and then executed before the next increment is combined.

18. A method according to claim 17, wherein the encryption step comprises encryption only of the instructions or op-codes of the program, data or operands remaining as plain text, and wherein execution of the program includes determining which signals fed to the tamper-resistant module are program instructions, and activating means for combining incoming signals with the memory map only when the incoming signals are determined as representing a program instruction.

19. A method according to claim 16, further including the steps of encrypting the key prior to storing the encrypted program and the key, and decrypting the key in the tamper-resistant module prior to generating the decrypted program copy.

20. A method according to claim 19, wherein encryption of the key is performed using a public key system, an auxiliary public key being stored in the external memory, and an auxiliary private key corresponding to the public key being stored in a second decryption memory in the tamper resistant module for decrypting the first mentioned key.

21. A method according to claim 20, wherein the program is encrypted using the DES algorithm and the key for generating the decrypted program copy is itself encrypted using the RSA public key system.

22. A method according to claim 21, wherein the encryption step includes using the DES algorithm in the cipher feedback mode.

23. Computer data processing apparatus constructed and arranged substantially as herein described and shown in the drawings.

24. A method of inhibiting the copying of or tampering with a computer program substantially as herein described.

Printed for Her Majesty's Stationery Office by the Courier Press, Leamington Spa, 1984. Published by the Patent Office, 25 Southampton Buildings, London, WC2A 1AY, from which copies may be obtained.